Report

Using ICT & Social Media in Disasters: Opportunities & Risks for Government Background Document

Author(s):
Giroux, Jennifer; Roth, Florian; Herzog, Michael

Publication Date:
2013

Permanent Link:
https://doi.org/10.3929/ethz-a-009920641

Rights / License:
In Copyright - Non-Commercial Use Permitted
Using ICT & Social Media in Disasters: Opportunities & Risks for Government

Background Document

Zurich, February 2013

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)
CONTENTS

1. INTRODUCTION: DEFINING TERMS & SCOPE OF STUDY .............................................. 4

2. SOCIAL MEDIA: COMMUNICATING RISKS & DEALING WITH CRISIS ......................... 9
   2.1 Monitoring & situational awareness ................................................................. 9
   2.2 Public safety and preparedness ....................................................................... 12
   2.3 Emergencies warnings, alerts and requests for assistance ............................... 15
   2.4 Recovery efforts ............................................................................................. 18

3. SUMMARY OF KEY FINDINGS ................................................................................. 20

4. BIBLIOGRAPHY ....................................................................................................... 23
   4.1 Websites ......................................................................................................... 26
INTRODUCTION: DEFINING TERMS & SCOPE OF STUDY

As Hurricane Sandy struck the US East Coast in October 2012, Internet usage in the region increased by 114%, with people turning to Twitter, Facebook, Reddit, and other social media platforms to retrieve and share information. Within the first 24 hours of the storm, over one million people mentioned the word “hurricane” on Twitter, Facebook was inundated with “Sandy” postings, ten storm-related pictures were posted per second on Instagram, and Internet-based chatting services like Skype saw a huge spike in traffic (Skype alone reported a 122% jump) both during and after the storm.

Illustrative of how this information sharing transformed into community action, tweets mentioning the Red Cross increased by thirty fold between 27 – 30 October 2012 as people sought ways to make donations and assist victims. Such activities were not simply limited to the general public; government officials, such as New York City Mayor Michael Bloomberg as well as Newark Mayor Cory Booker, used Twitter as a medium to communicate crisis preparation and response efforts, while private actors such as Google set up a dynamic crisis mapping platform and electricity provider Con Edison used Twitter to provide service updates to customers. Clearly, social media and information communication technologies (ICT) played a tremendous role in how people dealt with this crisis.

Yet, there is an important caveat to the Sandy case as not all information shared was accurate. As the storm made landfall, Twitter and Facebook were flooded with doctored or photo-shopped pictures. For example, one manipulated photo showed storm clouds gathering over New York that was actually a composite image of the New York harbor and a 2004 photo of a completely different storm that occurred in Nebraska. Another image was a still shot from the 2004 film The Day After Tomorrow with a NY1-TV logo superimposed on it. Pushing back against the spread of rumors and misinformation, the New York Fire Department used Twitter to post the message: “There is much misinformation being spread about #Sandy’s impact on #NYC” and also continuously reminded people to use official city Twitter feeds for accurate information. In another telling example that also shows how false information released through social media can be picked up by mainstream/traditional media, Twitter user @comfortablysmug posted a message that the New York stock exchange was flooded with water. CNN picked up this story after several local New York

“During an emergency, information is like gold”
Gail McGovern, president of the American Red Cross

---

2 More than 20 million tweets were sent containing the words “Sandy” and “hurricane,” as well as the hashtags #sandy and #hurricane between 27 October and 1 November. Laird, S. Sandy Sparks 20 Million Tweets, Mashable, 2 November 2012. http://mashable.com/2012/11/02/hurricane-sandy-twitter/.
4 See: http://google.org/crisismap/2012-sandy.
5 Many of those without power (electricity) still had access to mobile phones.
6 For a list of such photos see: http://urbanlegends.about.com/od/naturalwonders/ss/Fake-Hurricane-Sandy-Photos.htm.
City media outlets shared the post (or in the parlance of Twitter “re-tweeted” it); however, it soon realized that the story was in fact false.

This case is interesting as it reveals how the use of social media and ICT, particularly in crisis situations like Hurricane Sandy, exposes both the opportunities and risks that come with these new communication channels. Notably, it shows how information, whether it is accurate or false can go viral – moving quickly across different networks and social media platforms. Government actors are thus confronted with a rather challenging role: to both facilitate the spread of accurate information and leverage social media to reach the public through various channels, while also confronting the issues that arise when false or contradictory information emerges. Rather than fighting this trend (i.e. the use of ICT in crisis), government actors are in an excellent position – as information sources and trusted authorities – to nurture and facilitate the use of social media and strengthen communication strategies by factoring in these new information pathways.

Given such shifts, citizens increasingly expect governmental agencies to use online media for two-way public communication. For example, following a recent survey from Germany, only 29% of respondents see sufficient opportunities to communicate online with authorities, while 35% of the respondents find that too few opportunities exist. Within risk communication (non-crisis), government actors can leverage social media to provide information through multiple channels while also building and fortifying relationships with the public. During a crisis, these channels become an important place to not only release or share accurate information, but to also quickly counter rumors and false information, as demonstrated by the New York Fire Department. Yet, despite these benefits, authorities also need to be aware that engaging in such communication channels has profound consequences since it can generate unexpected or unwelcome feedback, particularly if sound social media policies or guidelines are not in place.

Traditional media such as television and newspapers continue to play a prominent role in daily life and certainly during disasters. Though these media represent the old communication paradigm, one that is characterized by one-way information dissemination. Today’s world is much more complex, with information moving in multiple directions resulting in a dynamic process of two-way communication that allows for information to originate from and move through multiple and varied sources. A key driver of this trend is the advent of ICT in general and, within that, the emergence of social media. ICT refers to technologies that provide access to information via the Internet, wireless networks, cell phones, and other communication media. Social media can be understood as communication services that employ interactive online ICT (often referred to as Web 2.0 technologies) to enable the exchange of user-generated content. Social media are highly interactive “digital tools that feature content users may generate, manipulate, or influence.” In other words, social media encourages interaction and dialogue between users, creating an information space that is decentralized and devoid of hierarchy. Table 1 lists the various types of social media, such as forum and blogs, and offers examples of each.

---

8 To build a trust relationship with the public it is important to communicate through these channels not only during crisis situations, but also for regular communication purposes.


In addition, the legal and political frameworks within this space are in their infancy and still being debated. As a recent workshop on social media during crisis revealed:

“To a certain extent, the community finds itself in a “Wild West” situation, as the available technology has surpassed the rules and guidance that are currently in place. The resulting environment is particularly unsettling for individuals who are unfamiliar with this new space, causing them to opt out for the time being. However, even in the absence of clarity, it is imperative to use and experiment with the technology. Early adopters and champions of the technology will inevitably help to shape the tenor of laws, policies, and guidance.”

Table 1: Social media categories and examples

<table>
<thead>
<tr>
<th>Social Media</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forums</td>
<td>LiveJournal, Gutefrage, symptome.ch</td>
</tr>
<tr>
<td>Blogs &amp; Micro-blogs</td>
<td>Blogger, WordPress, Twitter, Tumblr, Sina Weibo</td>
</tr>
<tr>
<td>Photo/Video/Audio sharing</td>
<td>Instagram, Picasa, Flicker, Youtube, Pinterest</td>
</tr>
<tr>
<td>Chat/texting</td>
<td>Skype, BBM, Google chat, Whatsapp</td>
</tr>
<tr>
<td>Wiki's</td>
<td>Wikipedia, Wikitravel,</td>
</tr>
<tr>
<td>Networking</td>
<td>Facebook, LinkedIn, Google+, Xing</td>
</tr>
<tr>
<td>Rating/Reviews</td>
<td>Yelp, Trip Advisor, Klinik-Bewertungen.de</td>
</tr>
<tr>
<td>Bookmarking</td>
<td>Del.icio.us, Diigo, Digg, StumbleUpon, Mister Wong</td>
</tr>
<tr>
<td>Discovery engines &amp; news</td>
<td>RSS, Reddit, Slashdot</td>
</tr>
<tr>
<td>Crowdsourced maps</td>
<td>OpenStreetMap, Google Mapmaker, Ushahidi</td>
</tr>
</tbody>
</table>

However, social media represents a very dynamic and, still rather new field or technique of communication. While defining ICT and social media and distinguishing between the various types of platforms may be easy enough, the social behaviors expressed within them continue to unfold and reveal themselves in new and emergent ways. For example, when Facebook first emerged among a network of university students, people chalked it up to being a site for people to engage in relatively personal behavior such as connecting with friends, sharing photos, etc. Over time, however, its utility has transformed. For example, after a tornado devastated Joplin, Missouri, on 22 May 2011, a Facebook page named “Joplin, Mo. Tornado Recovery” was created and soon had 123,000 members. The goal of this page was to mobilize support for survivors and help locate family members. In fact, looking across the social media space, the behaviors and needs that people express during crisis are varied and continue to evolve. The following points are a summary of some of the main motivating factors.  

- Convenience
- Based on social norms
- Network/recommendations
- Humor & levity

In addition, access to current, filtered & unfiltered information
- Determine disaster magnitude
- Check in with family & friends
- Self-mobilize (donate, volunteer)
- Maintain a sense of community
- Seek emotional support & healing


More specifically, the ethical and internal guidelines for using social media are a prominent concern within governments. This includes developing a social media strategy that outlines what platforms or tools to utilize (such as creating a Twitter account for a public agency), how to use those platforms (terms of use, its purpose and how it connects to agency message or brand, etc.), identifying a social media spokesperson (who posts, determines what they post and how they respond to rumors/false info), identifying what comments (if it is a platform like Facebook) will be removed. These considerations will be discussed in the concluding section. They represent just a few of those deliberations that need to be clarified before an agency decides to use social media.

In addition, there is also a need to offer employee training so to imbue staff with the knowledge they need to interact with the social media space – both within and outside of their official capacity. For example, in 2012, three Welsh government civil servants were given warnings for misusing social media, with one posting political comments on Facebook, another commenting on government policy on Twitter, and a third commenting on a consultation on a government bill (also on Twitter). These cases bring to light the fact that employees are on the frontline of the social media space, and their engagement with it is not without risks. Without staff training and policy clarification and cohesion, the risks of using social media increase and can potentially lead to misinformation and unauthorized leaks of sensitive information from government sources, thus creating an unfavorable public relations or crisis communication scenario. The US Centers for Disease Control and Prevention has more than 1.3 million followers on Twitter (@CDCemergency). It uses this space as a primary channel for the agency’s communications with the public. But this is not an un-regulated practice – rather it is executed by trained staff that follows a social media guide, which includes a detailed process for tweets that usually have to be approved by standard clearance channels.

Examining the risks and opportunities for use of ICT and social media is particularly relevant for a country like Switzerland where statistics show that Internet usage is above 80%, and of those 55% use the Internet to obtain health information, while 36% of the Internet users also have a social network account. As of 2012, there were nearly 3 million Facebook users and 500,000 twitter accounts in Switzerland, one of which includes the WEF/Davos Twitter feed with well over 2 million followers. In addition, just as ICT and social media have played an increasingly important role in situations like Hurricane Sandy, the 2010 earthquake in Haiti and the 2011 earthquake/tsunami in Japan, to name a few examples, it is also finding a place in the Swiss context. Early adopters of social media in Switzerland (within the realms of crisis and risk management) include the Swiss Federal Nuclear Safety Inspectorate (ENSI), the Swiss Federal Office for Civil Protection (FOCP), and the Federal Office for Combating Money Laundering (MEL). The Swiss Federal Office for Combating Money Laundering (MEL) has more than 33,000 followers on Twitter (@MEL_Schweiz). It uses this space as a primary channel for the agency’s communications with the public. But this is not an un-regulated practice – rather it is executed by trained staff that follows a social media guide, which includes a detailed process for tweets that usually have to be approved by standard clearance channels.

Examine the risks and opportunities for use of ICT and social media is particularly relevant for a country like Switzerland where statistics show that Internet usage is above 80%, and of those 55% use the Internet to obtain health information, while 36% of the Internet users also have a social network account. As of 2012, there were nearly 3 million Facebook users and 500,000 twitter accounts in Switzerland, one of which includes the WEF/Davos Twitter feed with well over 2 million followers. In addition, just as ICT and social media have played an increasingly important role in situations like Hurricane Sandy, the 2010 earthquake in Haiti and the 2011 earthquake/tsunami in Japan, to name a few examples, it is also finding a place in the Swiss context. Early adopters of social media in Switzerland (within the realms of crisis and risk management) include the Swiss Federal Nuclear Safety Inspectorate (ENSI), the Swiss Federal Office for Civil Protection (FOCP), and the Federal Office for Combating Money Laundering (MEL). The Swiss Federal Office for Combating Money Laundering (MEL) has more than 33,000 followers on Twitter (@MEL_Schweiz). It uses this space as a primary channel for the agency’s communications with the public. But this is not an un-regulated practice – rather it is executed by trained staff that follows a social media guide, which includes a detailed process for tweets that usually have to be approved by standard clearance channels.


Air Rescue Service (Rega)\(^9\) as well as the Institute for Snow and Avalanche Research (SLF).\(^{10}\) Each organization manages social media accounts and provides RSS feeds. Rega and SLF have gone as far as to develop Apps (short for applications) for mobile online devices to enable users to make emergency requests and/or access safety information.

Given these trends, it is important to examine the various ways in which social media is utilized in risk and crisis communication. To do this, the following section will look at four different issue areas to analyze how social media is used in the context of risk and crisis communication. These areas include: public safety and preparedness; emergency warnings, alerts and requests for assistance; recovery efforts; and, finally, monitoring and situational awareness. In the context of each of these areas, we highlight the key literature and real-life examples to explore the risks vs. opportunities in the utility of social media. These four areas capture the role of engagement and strategy in both the risk and crisis space.\(^{21}\) In other words, debating the use of social media should not only be a conversation regulated to the confines of crises or disasters, but should also encompass the utilization of those spaces and engage the world of social media outside of crisis situations.

---


2 SOCIAL MEDIA: COMMUNICATING RISKS & DEALING WITH CRISIS

The expectations of the public are changing in today’s dynamic communication space, where people have access to multiple and overlapping information channels. When a crisis is unfolding, people no longer wait for an official statement from government actors; rather they turn to the news media, they go to Twitter or Facebook, they log onto forums and blogs, etc., because they expect information and they can get it quickly from various sources. What government actors cover is not only information, but also verification of the info, which the public values. However, in such a dynamic information environment, if a government lacks a policy on how to use social media, particularly in crisis situations (meaning it does not act, or act appropriately), then it may face a loss of credibility and struggle with the management of a crisis. To get ahead of this curve, debating the risks and opportunities of using social media is a critical first step to building a sound social media policy and identifying certain engagement guidelines. This section begins by looking at the role of social media in monitoring and building situational awareness.

2.1 Monitoring & situational awareness

In recent years, private business organizations as well as governmental agencies have increasingly discovered social media as a resource to monitor the organizational environment, the findings of which can inform communication strategies. Among professional risk and crisis communicators it can almost be considered a truism that successful risk and crisis communication requires a good knowledge about the information needs and feelings of the target audience. Therefore, two-way exchange is a key resource for crisis management organizations. Monitoring social media is a convenient and relatively cheap option for organizations to increase their understanding of the needs, interests and sentiments of the public within different contexts. For example, monitoring technologies can be used to identify crisis-related issues that are debated in online forums or social networks and develop a response. In this context, social media can be particularly useful to manage rumors and to correct public misinformation about a risk or a crisis event. Moreover, social media can be effective to evaluate an organization’s communication strategy. Monitoring public discourses on social media can contribute to answer key questions of organizational communication, such as “is our risk message understood by the audience?” or “why do many people not respond to a crisis according to our advice?” Since social media can be monitored mostly in real time, communication strategies can be adapted very quickly.

Probably the most obvious way for governmental organizations to monitor social media is to create an online presence, for example on Facebook and Twitter, or by creating an organizational blog. Since all these media formats are reciprocal (*i.e.* they allow other users to comment), they can function as important sources for organizations to learn about their environment. To this end, as mentioned in section 2.1, FEMA not only created a Facebook page, but also has

---


a regularly updated blog that attempts to blend interesting emergency-related stories with useful public communications. This engaging style attempts to bring about regular visitors who are neither immediately concerned with emergencies nor professionals in the field. The ability to comment on entries is an important communication tool that allows FEMA “to have an ongoing conversation with all [their] stakeholders before, during, and after a disaster.” Finally, FEMA started a personal blog for its Director, Craig Fugate, to personalize the public communication of the organization (see Image 1).

Obviously, it is impossible for any organization to monitor all risk and crisis-related communication that occurs in social media spaces, particularly not during times of emergency. In order to manage the torrent of information transfer during times of disaster, in recent years various social media monitoring software tools have been developed. For example, tools such as ‘Radian6’, ‘Sprout Social’ or ‘Buzzmetrics’ allow users to monitor the use of predefined keywords or analyze the valence of messages. Yet, these tools not only allow trends to be followed in online communication flows, but provide insights into demographic characteristics of social media users, their geographical location and even into relationships between users, which can be used to identify the most relevant groups in the organizational communication environment. Other software tools, such as NodeXL, enable network analyses and visualization of social media data.

While monitoring social media is already an established routine in many organizations, a rather recent trend is to utilize information gained from social media in crisis management processes directly. For example, crisis and emergency management organi-

---

26 See: http://www.fema.gov/blog.


28 See: http://nodexl.codeplex.com/
organizations are integrating social media into situational awareness systems, which are increasingly being used in crisis situations.\textsuperscript{29} For instance, the software company ‘Twitcident’ tracks dynamics in social media in real time, making it an integral part of crisis management.\textsuperscript{30} Such efforts are supported by recent studies that show how geo-referenced twitter messages often have a high accuracy that allows them to be used for situational preparedness purposes. A recent study that compared Twitter messages with official flood maps in the UK concluded that “[a]s ever more people take to social media to share and communicate, we are seeing that the data shadows of any particular story or event become increasingly well defined. (…) physical phenomena like hurricanes and floods don’t just leave physical trails, but create digital ones as well.”\textsuperscript{31} The activities of the Social Media Digital Operations Center (of the American Red Cross) are an example where an organization is actively integrating social media into situational awareness structures and does so with the support of the IT company, Dell. Additionally, the Operations Center uses Radian6 to integrate social media into its relief management efforts.\textsuperscript{32}

It is important to note that integrating social media into situational awareness does not come without challenges. First of all, despite the multitude of tools available, the integration of different data types into situational awareness systems, which are increasingly being used in crisis situations.\textsuperscript{29} For instance, the software company ‘Twitcident’ tracks dynamics in social media in real time, making it an integral part of crisis management.\textsuperscript{30} Such efforts are supported by recent studies that show how geo-referenced twitter messages often have a high accuracy that allows them to be used for situational preparedness purposes. A recent study that compared Twitter messages with official flood maps in the UK concluded that “[a]s ever more people take to social media to share and communicate, we are seeing that the data shadows of any particular story or event become increasingly well defined. (…) physical phenomena like hurricanes and floods don’t just leave physical trails, but create digital ones as well.”\textsuperscript{31} The activities of the Social Media Digital Operations Center (of the American Red Cross) are an example where an organization is actively integrating social media into situational awareness structures and does so with the support of the IT company, Dell. Additionally, the Operations Center uses Radian6 to integrate social media into its relief management efforts.\textsuperscript{32}

It is important to note that integrating social media into situational awareness does not come without challenges. First of all, despite the multitude of tools available, the integration of different data types into situational awareness systems, which are increasingly being used in crisis situations.\textsuperscript{29} For instance, the software company ‘Twitcident’ tracks dynamics in social media in real time, making it an integral part of crisis management.\textsuperscript{30} Such efforts are supported by recent studies that show how geo-referenced twitter messages often have a high accuracy that allows them to be used for situational preparedness purposes. A recent study that compared Twitter messages with official flood maps in the UK concluded that “[a]s ever more people take to social media to share and communicate, we are seeing that the data shadows of any particular story or event become increasingly well defined. (…) physical phenomena like hurricanes and floods don’t just leave physical trails, but create digital ones as well.”\textsuperscript{31} The activities of the Social Media Digital Operations Center (of the American Red Cross) are an example where an organization is actively integrating social media into situational awareness structures and does so with the support of the IT company, Dell. Additionally, the Operations Center uses Radian6 to integrate social media into its relief management efforts.\textsuperscript{32}

It is important to note that integrating social media into situational awareness does not come without challenges. First of all, despite the multitude of tools available, the integration of different data types into situational awareness systems, which are increasingly being used in crisis situations.\textsuperscript{29} For instance, the software company ‘Twitcident’ tracks dynamics in social media in real time, making it an integral part of crisis management.\textsuperscript{30} Such efforts are supported by recent studies that show how geo-referenced twitter messages often have a high accuracy that allows them to be used for situational preparedness purposes. A recent study that compared Twitter messages with official flood maps in the UK concluded that “[a]s ever more people take to social media to share and communicate, we are seeing that the data shadows of any particular story or event become increasingly well defined. (…) physical phenomena like hurricanes and floods don’t just leave physical trails, but create digital ones as well.”\textsuperscript{31} The activities of the Social Media Digital Operations Center (of the American Red Cross) are an example where an organization is actively integrating social media into situational awareness structures and does so with the support of the IT company, Dell. Additionally, the Operations Center uses Radian6 to integrate social media into its relief management efforts.\textsuperscript{32}

It is important to note that integrating social media into situational awareness does not come without challenges. First of all, despite the multitude of tools available, the integration of different data types into situational awareness systems, which are increasingly being used in crisis situations.\textsuperscript{29} For instance, the software company ‘Twitcident’ tracks dynamics in social media in real time, making it an integral part of crisis management.\textsuperscript{30} Such efforts are supported by recent studies that show how geo-referenced twitter messages often have a high accuracy that allows them to be used for situational preparedness purposes. A recent study that compared Twitter messages with official flood maps in the UK concluded that “[a]s ever more people take to social media to share and communicate, we are seeing that the data shadows of any particular story or event become increasingly well defined. (…) physical phenomena like hurricanes and floods don’t just leave physical trails, but create digital ones as well.”\textsuperscript{31} The activities of the Social Media Digital Operations Center (of the American Red Cross) are an example where an organization is actively integrating social media into situational awareness structures and does so with the support of the IT company, Dell. Additionally, the Operations Center uses Radian6 to integrate social media into its relief management efforts.\textsuperscript{32}

It is important to note that integrating social media into situational awareness does not come without challenges. First of all, despite the multitude of tools available, the integration of different data types into situational awareness systems, which are increasingly being used in crisis situations.\textsuperscript{29} For instance, the software company ‘Twitcident’ tracks dynamics in social media in real time, making it an integral part of crisis management.\textsuperscript{30} Such efforts are supported by recent studies that show how geo-referenced twitter messages often have a high accuracy that allows them to be used for situational preparedness purposes. A recent study that compared Twitter messages with official flood maps in the UK concluded that “[a]s ever more people take to social media to share and communicate, we are seeing that the data shadows of any particular story or event become increasingly well defined. (…) physical phenomena like hurricanes and floods don’t just leave physical trails, but create digital ones as well.”\textsuperscript{31} The activities of the Social Media Digital Operations Center (of the American Red Cross) are an example where an organization is actively integrating social media into situational awareness structures and does so with the support of the IT company, Dell. Additionally, the Operations Center uses Radian6 to integrate social media into its relief management efforts.\textsuperscript{32}

It is important to note that integrating social media into situational awareness does not come without challenges. First of all, despite the multitude of tools available, the integration of different data types into situational awareness systems, which are increasingly being used in crisis situations.\textsuperscript{29} For instance, the software company ‘Twitcident’ tracks dynamics in social media in real time, making it an integral part of crisis management.\textsuperscript{30} Such efforts are supported by recent studies that show how geo-referenced twitter messages often have a high accuracy that allows them to be used for situational preparedness purposes. A recent study that compared Twitter messages with official flood maps in the UK concluded that “[a]s ever more people take to social media to share and communicate, we are seeing that the data shadows of any particular story or event become increasingly well defined. (…) physical phenomena like hurricanes and floods don’t just leave physical trails, but create digital ones as well.”\textsuperscript{31} The activities of the Social Media Digital Operations Center (of the American Red Cross) are an example where an organization is actively integrating social media into situational awareness structures and does so with the support of the IT company, Dell. Additionally, the Operations Center uses Radian6 to integrate social media into its relief management efforts.\textsuperscript{32}

It is important to note that integrating social media into situational awareness does not come without challenges. First of all, despite the multitude of tools available, the integration of different data types into
a single information system can be technically demanding and is currently a practice in its infancy. Beyond these rather technical challenges, a more fundamental problem could occur if situational awareness processes would be misled by flawed information from social media. As a recent study on Twitter use during floods in Thailand highlights, “[i]nformation that is false, outdated, or inaccurate could complicate situational awareness of a crisis and hence slow down relief efforts. For example, if the government plans to implement social media as a tool for disaster response, it would be well advised to prepare some measures or protocols that help officials verify incoming information and eliminate false information.” Finally, the use of social media for situational awareness could possibly raise privacy issues. Even if the monitored data is public communication, citizens potentially could get afraid of state authorities playing “big brother”. To avoid such allegations, authorities can clarify how they collect, store, use and forward information gained from social media monitoring. As an example, the U.S. Department of Homeland Security has issued a notice that it would forward Personally Identifiable Information (PII) to responding authorities only “in the event of an in extremis situation”.

### 2.2 Public safety and preparedness

Ensuring or enhancing public safety and communicating risks is a constant process for government. As Coyle and Meier state in a 2009 report: “Meeting the information needs of communities before the onset of emergencies is an important way to build preparedness and resilience.” While resilience connotes the sustained ability of a system to withstand and recover from adversity, it takes an informed, connected and resourceful community to deal with and adapt to shocks. Thus, the process inherent in preparing the public and raising risk consciousness is not hindered, but rather benefits from the multiple information and communication channels offered through ICT tools and the interactive nature of social media. It broadens the space in which government actors can reach out and engage the public, essentially creating a more nuanced approach that allows for customizable communication strategies to reach target groups.

In terms of specific opportunities, using social media as part of risk communication and preparedness efforts is an excellent way to reach various segments of the population – particularly younger people, most of whom use such tools as a key source of information. In fact, looking at the statistics in the United States alone, a 2012 study carried out by Pingdom examined 24 popular online social media communities in (the US) and found that 51% of users are between 25 and 44; 21% are age 24 and younger; and 27% are age 45 and older. To be clear, these are general statistics, not tied specifically to a crisis situation and they are also from a country outside of the European context. But nevertheless their findings are relevant to this context.”

---


discussion. Pooled together, the average age is 37. Those over 55 tend to rely more on traditional media sources (newspapers, television) as their primary source of information. Needless to say, such studies reveal the importance of using different types of media to reach out to various parts of society. They also show how, for the younger generations, social media is playing a major role in all facets of their professional and personal life.

Rather than waiting for a crisis to strike and then using social media to liaise with the public, it would behoove government actors to begin incorporating such tools into regular exchanges with the public as it provides the space to link into and build a network – for example followers on Twitter or members on a Facebook group. Developing such a network during a crisis, certainly when time pressure is high, is not typically a top priority.39 Or as Sergeant Sean Whitcomb of the Seattle Police Department explained at a workshop on social media use: “Establishing the brand when things are slow will help when things turn hectic.”40 In the best case, active engagement with social media can help to increase public trust in a government agency or, more specifically, crisis management organization, which in turn is a key resource for successful risk and crisis communication.41

As the experiences in different countries show, social media can be used in multiple ways to support public risk communication and increase social preparedness: In the United States, the Federal Emergency Management Agency (FEMA) launched the “Severe Weather Week” campaign which aims to inform and encourage people to take precautionary measures against destructive weather phenomena.42 In the spirit of resilience building, this campaign sought to encourage the development of emergency plans within families, noting that “individuals can contribute to preparing themselves and their community for severe weather in their area.” This proactive campaign is an example of some of the preparedness efforts that can then be promoted and communicated across various platforms. On FEMA’s website, where it announces the campaign, it also references five different social media sites where people can follow FEMA’s work and activities (see image 3). FEMA’s Facebook page communicates such messages and activities to its 124,000 members (at the time of writing).43 The site is highly interactive, featuring pictures and videos from the field, comments and discussions from members, and allowing for a two-way exchange between a government agency and the public – a more effective mechanism than top-down approaches.44

43 See: https://www.facebook.com/FEMA.
as well as to showcase interactions with the public, experts, etc. For example, they share videos that feature interviews with scientists and other people on health-related topics. In Norway, the Oslo Police District has established a Twitter service that mainly provides information about recent police operations, but is also regularly used for risk communication purposes. In January 2013, the account won the Norwegian “Tweet of the Year” competition, mainly due to its personal and sometimes also humorous tone. In Australia, the Country Fire Authority (CFA) has specifically designed a game for children which teaches them how to evacuate their homes in case of a fire emergency and uses social media platforms as a way to enhance the audience reach. Finally, the Swiss Institute for Snow and Avalanche Research (Institut für Schnee- und Lawinenforschung, SLF) offers the

---

For a full list of social media sites see: [http://www.epa.gov/epahome/socialmedia.html](http://www.epa.gov/epahome/socialmedia.html)

[45]

“White Risk” app (provided in German, French, Italian and English), which is not particularly interactive, but rather a platform for users to access information on mountain conditions (snow and weather) as well as to assess the avalanche danger via the Danger Analyser, which helps users evaluate conditions and make informed risk-related decisions (Image 4).

These examples illustrate the ways in which social media can be used for public safety and risk communication. Certainly, they can help create awareness, as illustrated in the “White Risk” app, or promote preparedness efforts, as demonstrated by FEMA’s efforts. Combined, such efforts can result in a more aware and prepared public that can then feed into crisis/disaster management efforts, mitigating adverse impacts (i.e. faster recovery). It is also worth highlighting that such examples showcase the ways in which governments are leveraging social media platforms to expand the reach of “conventional” media messages like videos, leaflets, information brochures, pictures and even games. Of course, using these platforms opens up the possibility of people commenting and interacting with these messages and also spreading the risk messages through their (personal) networks, which are often comprised of trusted sources such as friends or neighbors.47 In other words, e.g. an emergency preparedness guideline shared by a good friend on Facebook will increase and multiply its reach.

At the same time, some risks need to be considered, when using social media to disseminate public safety and preparedness information. Arguably, the most significant risk is the lack of a social media policy or strategy, as discussed in the previous section. There must be clear guidelines in place to guide this process, as well as trained professionals to manage the presence on various social media platforms. Given the quick interactive nature of social media platforms, government actors that do not engage the social media space or fail to provide regular postings and responses to public interactions, will risk their credibility. As Einhorn explains “the public (including the news media) now expects to be able to find official government information on social media. Any agencies that are still treating their Facebook, Twitter and other social accounts as untended gardens will face an increasingly frustrated constituent base.”48 A social media policy/strategy, as well as the appropriately designated manpower, will help avoid this risk.

Another consideration is the risk of sending out mixed messages. Utilizing more media platforms and tools to communicate to the public does not necessarily mean sending out different risk messages, but rather it’s about extending the reach of those messages and creating an echo effect. Of course, communication in social media has to be coordinated with the information activity on other platforms – and while different media channels can be used to communicate with different tones, the central messages should remain the same in order to keep up a “one voice” communication strategy. Given that messages sent out will likely render a response by users (i.e. the public), government actors should also coordinate responses. Uncoordinated responses to inquiries also raise certain risks, notably to credibility and impact of message dissemination.


2.3 Emergencies warnings, alerts and requests for assistance

This discussion will shift from a focus on communicating about risk to communicating in crisis and examine how social media can be used to communicate warnings and alerts as well as offer a space to request assistance in the case of emergencies. Obviously, these types of communications are more time sensitive and mistakes can have severe consequences. There are numerous examples of social media platforms being used by crisis and emergency response agencies. For example, the US Centre for Disease Control and Prevention uses Twitter as a platform to communicate disease-related warnings to the public.49 The American Red Cross has a Tornado App for Android and iOS, which provides alerts about tornado-related hazards and provides helpful information.50 Similarly, the US National Weather Service links the Tornado Watch to the Storm Prediction Center on Facebook (Image 5).51 Obviously, the usage of social media to alert the public to natural hazards is of great interest to many stakeholders as it can provide some extra time for people to take precautions and get to safety before the storm strikes.52

We also observe the growing role of social media in requests for (emergency) assistance. While using the telephone (whether it is a landline or mobile phone) is still a prominent and popular way to call for assistance, there is some indication that people would like additional means to alert authorities. For example, a study by the American Red Cross revealed that 69% of the US population thinks that emergency response organizations should regularly monitor and respond to postings on their websites.53 Along these lines, the London Fire Brigade is exploring ways to set up the world’s first 999 emergency Twitter feed, which would allow users to report fires and other incidents using their own Twitter accounts.54 Likewise, the US Federal Communications Commission (FCC) announced that the four major US mobile operators – AT&T, Verizon, Sprint and T-Mobile – have all agreed to create a text-to-911 technology, making it available in spring 2014.55

Providing ways for ICT and social media tools to be used by the public to alert authorities about emergencies offers individuals additional and sometimes more convenient options to request assistance. It also raises the transparency of requests – if a request is made over a platform like Twitter, it has a public audience to hold the emergency responder accountable. Confirming this perception, a 2010 study commissioned by the American Red Cross found that 49% of the 1,058 respondents believed that requests for assistance made to an emergency response organization had a higher chance of receiving a response if they were posted on a social media site.56

In terms of the use of social media to communicate emergency warnings and alerts, we identified three main opportunities. First, messages can quickly and easily reach a large audience as well as a certain in-
With regards to calls for assistance, many point to the risk of inaccurate or malicious information (spoofing) made via social media tools and the potential that such inaccurate reports will spread or be duplicated. A 2011 study illustrates these risks as it found that rescue efforts after the Japan tsunami disaster in Japan were hampered by misleading and confusing tweets by people requesting assistance.

However, even in the area of emergency calls, there are numerous cases of fake or false reports. See table 2 for a list of various European countries and the corresponding percentage of fake emergency calls they receive. This list was generated from a 2011 study conducted by the European Emergency Number Association (EENA). Austria for example reported that 30% of emergency (telephone) calls that they received were false or some type of a hoax.

Aside from these advantages, there are obviously also some risks. With regards to calls for assistance, many point to the risk of inaccurate or malicious information (spoofing) made via social media tools and the potential that such inaccurate reports will spread or be duplicated. A 2011 study illustrates these risks as it found that rescue efforts after the Japan tsunami disaster in Japan were hampered by misleading and confusing tweets by people requesting assistance. However, even in the area of emergency calls, there are numerous cases of fake or false reports. See table 2 for a list of various European countries and the corresponding percentage of fake emergency calls they receive. This list was generated from a 2011 study conducted by the European Emergency Number Association (EENA). Austria for example reported that 30% of emergency (telephone) calls that they received were false or some type of a hoax.

---


58 Lindsay (2011).
mental agencies have to consider the security risks of using social media, especially for critical communications like emergency warnings and alerts. If, for example, the social media account of the crisis management agency gets hacked, intruders could disseminate fraudulent information through this communication channel. This could have disastrous consequences. Fourth, the implications of two-way communication must be considered, for example verifying warnings by users etc. Overall, considerable risks exist, although – as is the case with the use of traditional media – they appear to be manageable so long as necessary efforts are made to understand and mitigate them.

2.4 Recovery efforts

The challenges in the aftermath of a disaster are manifold and information is a fundamental part of a quick recovery. Disaster information is as important as water and food. Organizations and people involved in the assistance efforts need to know where help is needed, how the aid can be brought to the people who need it and possibly also to counter further harm. Furthermore, a damage estimation is necessary, e.g. to request further help from other organizational and/or federal units and, in the worst case, from other countries.

What are the opportunities in the area of recovery efforts after an emergency incident in using social media? First, the damage assessment can be improved. One option is visualizing the crisis space using crisis mapping platforms. By generating crowd-sourced crisis maps of inflicted damage based on user reports (which are commonly uploaded via mobile phones), the damage response teams can manage the disaster more effectively and quickly. This broad information base adds valuable detection time, allows them to concentrate on actually dealing with the damage and also in assessing the need for any further assistance.

To mitigate these risks, government actors need to consider how they will treat requests for assistance made through social media platforms. For example, what will the verification procedures look like? Will they treat every report the same as if it came through via telephone, or will they triangulate information with other media and individual reports? Also, how will they manage issues related to reputation management, such as if a user posts negative information or feedback about the response or assistance efforts? In sum, government agencies must consider these risks and mitigate them by developing a system to verify the authenticity and respond in a timely and coordinated manner.

As for warnings and alerts, using social media must be coordinated with the general communication strategy. These alerts must be accurate and up-to-date, or else they lose their utility and credibility. In addition, because life and property can depend on this information, a strict “quality control” is necessary. This means that if social media sites are used as a communication channel for warnings and alerts, an adequately staffed and trained team is necessary to manage the system. A half-hearted approach will quickly become counter-productive and even increase the risks. Finally, govern-

---

63 Coyle and Meier (2009), p 17.
64 Homeland Security News Wire: How smartphones are fight-
Second, social media can help individuals with targeted recovery information. By using social media, governmental agencies can inform the public where they can get assistance according to their specific needs, how they can apply for disaster loans and generally offer help and information during the recovery phase. They can also support the broad request for donations to help the affected people by increasing the reach of the campaign by the aid agencies and making the process of donating easier. The American Red Cross for example offers donation possibilities through Facebook, as well as with their mobile app in the case of Hurricane Sandy.

Third, the use of social media platforms also encourages the self-organization of the affected population. Good examples of self-organization were the severe winter storms in the United States in 2010 (“Snowmageddon”, see Image 6) or the Russian Bushfires 2010 where crowd-sourced crisis maps were also used to coordinate recovery efforts by individuals. These examples illustrate that people can directly offer their help, like housing, food donations and other assistance, to the people affected by using these platforms. Such assistance can offset workload and resource demands placed on governments during crises, and also reduce the timeframe in which this support can be brought to bear for the affected individuals. It is also possible to use social media to find displaced people and property in the aftermath of a natural disaster, thereby also reducing the necessary resources of official disaster agencies.

Obviously, there are also risks in using social media platforms in the realm of recovery efforts after an emergency event. First, the self-help efforts by citizens can conflict, in the sense of duplication or mis-information, with the government response. For example, people creating Facebook groups offering information on lost persons or items may conflict with government efforts to do the same. Second, the risk of fraud and advantage-taking are a problem. In individuals could be tempted to take advantage of the situation and request more or other assistance than they actually need. This could damage other people in distress who would actually need the help more, but have lack of access to social media. Although this is a serious problem, it is not an exclusive aspect of using social media in the recovery efforts, but rather a common issue in every kind of emergency situation.

---

65 See: http://apps.facebook.com/redcross-donate/
68 See: http://www.russian-fires.ru/.
69 See Coyle and Meier (2009), chapter 5.
3 SUMMARY OF KEY FINDINGS

ICT in general and social media more specifically are an integral part of many people’s lives today, including during times of crisis. In the previous section, we discussed how governmental actors can participate, leveraging ICT and social media to improve risk and crisis communication efforts. As the different examples illustrate, already today crisis management authorities in many countries are using the new technologies to increase public awareness and preparedness for disasters, alert the public and optimize situational awareness when crises strike, and speed up recovery processes thereafter. Based on our analysis above, we find the following four overarching arguments that underscore the opportunities that ICT and social media can bring for governmental risk and crisis communication.

Opportunities

1. Employing state of the art ICT increases the range of governmental communication. Although social media will not replace traditional media in the foreseeable future, already today many young people heavily rely on social media to gain information, making this population hard to reach through established communication channels such as radio or television. While this trend will most likely continue in the coming years, it will be met with another trend where Western societies are aging. Therefore it is about striking a balance; if government concentrates too much on any one type of media (whether social or traditional), it will risk missing a part of the society. In other word, social media tools are only one of many communication tools to use.

2. Online ICT enable high-speed communication. Since during emergencies, most information for public communication such as evacuation orders or protection advice is highly time-sensitive, it should be used in combination with other communication tools. For example, siren alerts or alarms can alert the public at large while ICT and social media tools can provide another high-speed platform to deliver additional information. Although the speed of online communication sometimes makes it hard for governmental actors to catch up (for example if rumors spread), this should not be used as an excuse for refraining from ICT use for governmental communication, because otherwise misinformation spreads uncontrolled. To the contrary, governmental actors can use ICT like social media effectively to engage as misinformation or rumors unfurl and thereby contain their spread.

3. Online communication can be easily tailored towards individual needs. In comparison to many traditional media channels such as newspapers, radio or TV, online information services can theoretically contain almost unlimited amounts of information. Due to the interactive design of ICT, citizens can choose which risk or crisis information is most useful to them. For example, via ICT citizens are enabled to obtain disaggregated crisis information just for their geographic area. This way, social media and other online services can be highly target-group-specific, finally fostering social and individual self-efficacy.

4. Social media are social media. Contrary to the critical view that social media encourages, and is characterized by anonymity, the vast majority of communication in social media is identifiable. Just as in offline-communication, also online commu-
nication is about affinity, acquaintance and trust (often referred to as social capital). Professional crisis and risk communicators can leverage this social capital by feeding social media with authoritative risk or crisis information. If found relevant, this information then gets forwarded to other social media users, so social capital promulgates the sharing of information in the online socio-environment. In this way, risk and crisis information shared through social networks receives the attention (and arguably also trust) of more people, and, finally, also raises the chances for individual action as we have seen with the crisis mapping phenomenon. Government actors can also use social media to foster their own social relationships and build social capital with the public. Social media are particularly suited to two-way, long-term communication and engagement, which are commonly regarded as strong bases on which mutual trust is built. Consequently, the use of social media by government actors appears as a promising way to strengthen their relationships with key stakeholders as well as the general public.

Despite these different opportunities that new ICT such as social media are opening up for professional risk and crisis communicators, utilizing these tools should be done with caution. Based on our review, we identify three main points that government actors should consider before engaging in social media or any other online tool for public communication purposes.

### Risks to Consider

5. **Employing new communication channels requires a social media strategy.** Most public organizations already have refined information policies and communication strategies. In order to minimize the risk to lose “unity of voice”, when using social media or other ICT for organizational communication, any new communication channel needs to be integrated into an overall strategy for “streamlining communication processes both internally and externally.” This way, the dissemination of premature or inaccurate information can be avoided. Moreover, information policies have to be adapted to the specifics of the information age. For example, this includes clarifying liability issues and managing public expectations (e.g. what if an organization does not respond to emergency request? Are terms of service of commercial social media platforms compatible with national regulations?).

6. **Gearing up organizational communication is an investment.** For an individual, joining Facebook or Twitter is a cost-free decision that manifests itself as a hobby. For a crisis management organization, this is fundamentally different. When governmental actors open up new communication channels this creates new expectations among citizens in respect to the channels’ completeness, reliability and validity. In terms of technique, this

---


means organizations using ICT have to assure that the information infrastructure is robust and safety standards are sufficient, so that the risk of information delay or corruption or even system disruptions is minimized. Investments in human resources must also be considered. If authorities commit to two-way communication, but do not engage with the public (i.e. provide feedback), having a social media presence can become counterproductive. Particularly critical are crisis situations, when the communication staff of crisis management agencies is under high pressure (for example having to keep up internal coordination and handling inquiries from the mainstream media). In order not to neglect important online communication channels, sufficient human resources must be allocated to ensure functioning public communication via all channels. In addition, organizations can manage public expectations by releasing public statements, for example by stating explicitly the limits of their social media services (e.g. that the organization cannot reply or react to every single inquiry coming from the public, particularly not during crisis).

7. Certain risks remain. Even if sufficient technical and human resources are allocated to online communication and a comprehensive social media strategy is in place, this does not rule out that social media can sometimes work against the interest of governmental agencies. In general, two-way communication across the board decreases information control on the side of governmental authorities and therefore inherits the risk of losing information advantage and interpretational sovereignty. No democratic government actor can actually control social media (even authoritarian governments rarely succeed). Instead, governments need to acknowledge that due to the non-hierarchical architecture, social media can and sometimes will be used to disseminate dissonant, inaccurate or even malicious information. However, experiences indicate that at least inaccurate information can be corrected without significant damage through social media. The uncontrollable spread of misinformation (so-called “infodemics”) is the exception.

To be sure, the challenges and risks that are associated with the use of social media and other online ICT discussed in this report are not insurmountable. While the challenges of new communication channels should not be underestimated, if the implementation of these channels is accompanied by the necessary investments and strategic adaptations, there is no reason for governmental organizations to refrain from bring these tools into their overall communication strategy. In the long run, authorities will have no other choice than to “go where the people are” if they want to stay connected to their audiences.


BIBLIOGRAPHY


WEBSITES

This list contains some of the key sites/links referenced in this report

http://www.cio.com/article/701810/Dell_Powers_Red_Cross_Social_Media_Command_Center

http://google.org/crisismap/2012-sandy

http://urbanlegends.about.com/od/naturalwonders/ss/Fake-Hurricane-Sandy-Photos.htm

http://www.bbc.co.uk/news/uk-wales-21644757

http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/03/key/ind16.indicator.30106.160204.html

http://www.socialmediaschweiz.ch/Top_Twitter_Accounts_Schweiz_Marz_2012_.pdf

https://twitter.com/ensi_ch

http://www.youtube.com/user/ensitube/videos?sort=dd&flow=list&page=1&view=0

https://www.xing.com/companies/eidgen%25C3%252596ssischesnuklearsicherheitsinspektoratensi/updates

http://www.ensi.ch/en/feed/


http://www.facebook.com/rega1414

http://www.youtube.com/regatv

https://www.xing.com/companies/schweizerischerrettungsflugwacht

http://www.slf.ch/ueber/organisation/warnung_praevention/projekte/white_risk_mobile/index_EN

http://www.slf.ch/dienstleistungen/rss/index_DE


https://www.facebook.com/FEMA

http://thorne.ws/2013/02/06/oslo-police-district-won-tweet-of-the-year/
https://twitter.com/CDCFlu

http://www.redcross.org/mobile-apps/tornado-app


http://konradweber.ch/angebot/news-verifikation/

http://www.homelandsecuritynewswire.com/how-smartphones-are-fighting-floods

http://apps.facebook.com/redcross-donate/

http://www.imore.com/donate-red-cross-hurricane-sandy-relief-directly-app-store

http://nyc.snowmageddoncleanup.com/main

http://www.russian-fires.ru/

http://www.fema.gov/blog

http://www.salesforcemarketingcloud.com/products/social-listening/

https://sproutsocial.com/

http://nmincite.com/solutions/my-buzzmetrics/

http://nodexl.codeplex.com/


The Center for Security Studies (CSS) at ETH Zurich specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.